easyPRO Cyber pour les artisans

1. Pourquoi les artisans sont pris pour cible ?

Les cybermenaces ne concernent plus seulement les grandes entreprises ; elles touchent désormais les PME et les artisans. Chaque faille de cybersécurité est exploitée par les cybercriminels, souvent via des erreurs humaines (mot de passe faible, logiciel non mis à jour). Pour un artisan, les conséquences sont immédiates : un accès bloqué à la gestion de stocks, à la machine indispensable, aux devis, aux factures ou aux données clients peut suffire à stopper net l'activité. Au-delà du coût, c'est aussi la relation de confiance avec les clients et l'image de l'entreprise qui est fragilisée, sans compter les obligations réglementaires en cas de fuite de données.

29 jours

Le temps nécessaire à une entreprise pour retrouver son activité normale après une cyberattaque. (1)

60 %

des PME victimes d'une attaque majeure ferment en 18 mois.(2)

2. Exemple concret de cyberattaque

Un boulanger voit son activité brusquement paralysée par une cyberattaque. Ses systèmes sont bloqués, une rançon est exigée. Ses équipements automatisés et son four programmé dysfonctionnent, son système de caisse est à l'arrêt, et il n'est plus en mesure d'honorer ses commandes auprès des restaurants et hôtels. Résultat : une activité stoppée net, des pertes immédiates et des clients non servis.

Qu'aurait pris en charge l'assureur ?

Qu'aurait pris en charge l'assureur ? L'assurance easyPRO Cyber aurait pris en charge l'assistance d'urgence et la gestion de crise à hauteur de 5 000 €, les frais de reconstitution du système informatique à hauteur de 10 000 €, les pertes de marge brute d'exploitation liées à l'interruption de l'activité sur une période de 3 jours à hauteur de 7 500 €, ainsi que les frais de négociation de la rançon à hauteur de 3 000 €.

(1) Bessé et le Groupe Stelliant - 2023
(2) Hiscox Cyber Risk Study - 2023

3. Les principales conséquences d'une cyberattaque

Les cyberattaques réussies paralysent l'activité de l'artisan, entraînant une interruption totale ou partielle du système informatique.

- Arrêt de production : Les équipements automatisés (fours, mélangeurs) et les systèmes de gestion (caisse, stocks) sont bloqués, empêchant la production et la vente.
- Perte de revenus et clients : Impossibilité d'honorer les commandes (notamment les gros clients comme les restaurants), entraînant une perte de chiffre d'affaires immédiate et une perte de confiance de la clientèle.
- Impact réputationnel : La relation de confiance avec les clients est fragilisée, et l'image de l'entreprise est durablement atteinte

4. Ce qui est couvert par l'assurance easyPRO Cyber

ASSISTANCE ET EXPERTISE

Hotline d'urgence 24/7

Nous mettons à votre disposition un numéro d'appel d'urgence (+352 4761-4444) 24h/24 et 7j/7 pour missionner un expert de notre partenaire Dattak qui coordonnera la gestion de votre incident (sans franchise). Dattak déploie son réseau de plus de 50 experts cyber, juridiques et en gestion de crise qui interviennent pour sécuriser vos systèmes, gérer l'attaque et limiter les impacts sur votre entreprise.

Interventions d'experts

Nos meilleurs experts vous accompagnent : ingénieurs, experts en cybersécurité, experts juridiques, gestion de crise, etc.

Exemple : Votre commerce est victime d'une cyberattaque et votre réputation est fortement impactée. Nos experts en communication de crise vous assisteront dans la gestion des relations publiques et dans votre communication interne et externe.

RESPONSABILITÉ CIVILE

Responsabilité Civile Cyber & Média

Nous prenons en charge le coût et les frais de défense résultant de toute réclamation introduite par un tiers suite à une fuite de données et/ou une transmission de virus.

Exemple : Votre commerce est victime d'une cyberattaque et les données personnelles de l'un de vos clients fuitent ou vous transmettez un virus à un tiers. Il vous poursuit en justice pour obtenir un dédommagement. Nous prenons alors en charge tous les coûts et les frais de défense (gestion des réclamations, frais d'enquêtes, frais d'avocats, etc.)

DOMMAGES ET PERTES

Frais de monitoring et de surveillance

Nous prenons en charge les frais engagés pour détecter l'utilisation non conforme de données personnelles.

Exemple : Les données de vos clients fuitent et parmi ces données se trouvent des informations sensibles et/ ou des informations permettant d'identifier directement ou indirectement un client. Nous engageons alors des frais pour nous assurer que ces données ne sont pas utilisées à des fins malveillantes.

Frais de notification

Nous prenons en charge les frais de notification aux autorités et aux personnes concernées en cas de vol de données personnelles.

Exemple : Votre commerce est victime d'une cyberattaque, vous êtes alors dans l'obligation de notifier tous vos clients impactés par l'attaque ainsi que la CNPD.

DOMMAGES ET PERTES

Frais de reconstitution de vos données et de votre système informatique

Nous prenons en charge les frais de reconstitution des données présentes sur vos sauvegardes exploitables ainsi que les frais engagés pour remettre votre système informatique en bon état de marche.

Exemple : Suite à une cyberattaque, le système informatique de votre commerce est impacté. Nous prenons en charge tous les frais nécessaires à sa restauration dans le même état de fonctionnement que celui existant avant l'attaque.

Frais d'enquêtes et sanctions administratives

Nous prenons en charge les frais d'enquêtes diligentées à votre encontre par une autorité administrative ou gouvernementale compétente au titre de la violation des données personnelles ou suite à un manquement aux règles de sécurité PCI DSS (pour les cartes bancaires). Ainsi que les éventuelles amendes et pénalités dès lors qu'elles sont légalement assurables.

Exemple : Suite à une cyberattaque, des données personnelles de vos clients fuitent et la CNPD lance une enquête à votre encontre. Nous prendrons en charge les frais de défense dans le cadre de cette enquête.

Pertes d'exploitation

Nous prenons en charge vos pertes de marge brute d'exploitation consécutives à l'interruption totale ou partielle de votre système informatique.

Exemple : Votre commerce est victime d'une cyberattaque, vous êtes dans l'obligation d'interrompre totalement ou partiellement votre système informatique pour limiter les dégats. Nous prenons alors en charge vos pertes de marge brute d'exploitation. C'est à dire la marge brute que vous auriez dû réaliser sur la période d'interruption.

Frais de négociation de la rançon

Nous prenons en charge les frais de la négociation de la rançon.

Exemple : Votre commerce est victime d'une cyberattaque. Les malfaiteurs prennent le contrôle de vos données et exigent une rançon, tout en menaçant de publier des informations sensibles. Nous prenons en charge les frais de négociation de la rançon, notamment l'intervention d'experts spécialisés, et vous accompagnons à chaque étape pour gérer la situation et limiter les impacts.

Cyber-fraude

Nous prenons en charge les conséquences pécuniaires faisant suite à une cyber-fraude.

Exemple : Votre commerce est victime d'une cyberattaque, les malfaiteurs s'introduisent dans votre système informatique et envoient un mail à votre responsable financier pour qu'il émette un virement. Nous prenons alors en charge le montant des fonds détournés.

Surfacturation téléphonique

Nous prenons en charge les surcoûts dus à une utilisation frauduleuse de vos lignes téléphoniques.

Exemple : Votre commerce est victime d'une cyberattaque et les malfaiteurs utilisent vos lignes téléphoniques pour appeler des numéros surtaxés. Nous prenons alors en charge le surcoût.

DON'T WORRY be happy

lalux ASSURANCES